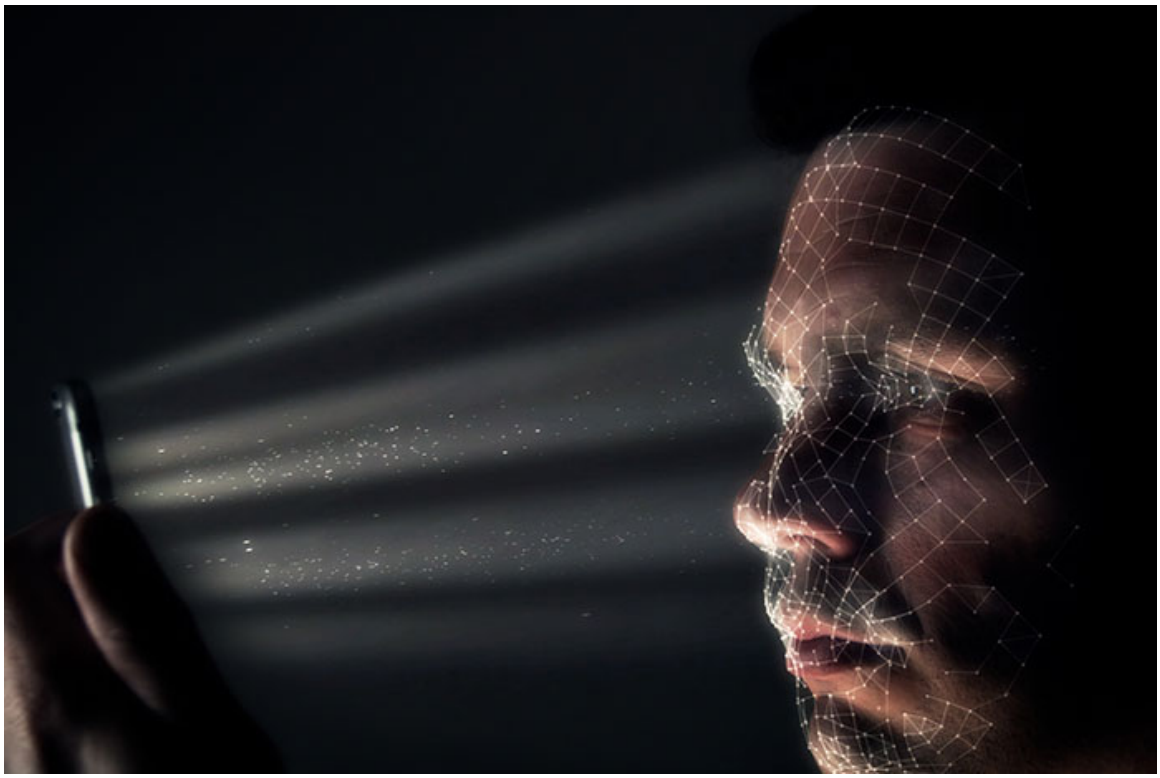
Facial Recognition From Multiple Sources

by dqr | Apr 20, 2018 | Research | 0 comments



Deborah Harmes, Ph.D.

Whether it is on new cameras or incorporated into software built atop the blockchain platform, new solutions – or potential intrusions – with facial recognition continue to arrive with increasing regularity.

The newest 'smart camera' technology has created cameras with an accuracy of 99.7% in their ability to correctly identify people's faces. Cloud-based image storage — uploaded by a group of camera manufacturers including Nikon, Sony, Wistron, Foxconn, and Scenera – is an essential part of an alliance called the Network of Intelligent Camera Ecosystem (NICE); the technology used by NICE cameras would recognise both faces and objects. MobileNets, created by Google and released in mid-2017, aims to continually improve the accuracy of their sensing within the small processing space of a mobile phone.

A similar type of facial recognition is necessary for identity verification and documentation. Biometrid has built a program called 'One Face, One ID' that is designed to help ensure that the correct identity is being presented when a variety of websites,

including banks and trading companies, require proof of identity prior to opening a new account. Biometrid's built-in safety factor includes the fact that blockchain records of identity are tamper-proof. With uses as diverse as normal laminated ID cards, verifying the identity of delivery personnel, purchasing cryptocurrency or stocks and shares, renting a car or apartment on holiday, or making plane or train reservations, more and more companies plan to require a secure identity check before they will do business with a new customer.

As the use of facial recognition technology increases each year, there are also people who have questioned the necessity and safety of so much observation in our daily lives. Apps have already been produced that allow you to pay for goods and services simply by having your face scanned, but is that a good thing? Somewhere, in some blockchain, your purchase records are being kept and potentially analysed. We've already seen how the recent Facebook scandal about information harvesting has unfolded – so imagine the amount of information that could be extrapolated from detailed consumer purchase records.

Additionally, there are also other worrying aspects of a non-stop increase in facial recognition technology. Some apps allow you to take a photo of someone, upload it to the app, and scan for that person's location via social media. Stalkers and criminals including thieves and child or spouse abusers could find and target people this way. Also, apps that interpret body language can assess an individual's vulnerability and potentially place that person in danger. Furthermore, apps that scan facial characteristics that appear in various diseases or mental health conditions can cause people to become labelled for life. In fact, the use of facial scanning to deny employment or judge personality based on some department's or person's definition of 'negative characteristics' has already unfolded in Shanghai and been immediately condemned.

While facial recognition software used in tandem with blockchain software can make our lives easier, the many vulnerabilities of this combination should be kept in mind.